第四次作业

- 分析环境

OS	Arch
Android 6.0	i686（4.0.9-android-x86+）
Android 6.0 (Linux kernel v3.10.0+)	armv7

- 使用工具

Tools	Version
Detect It Easy	v3.01
MuMu Player6.0	v2.7.34.0(x86)
MT Manager	v2.14.0
DnSpy	v6.1.8
IL2CppDumper	https://github.com/Perfare/Il2CppDumper最近更新于23-3-5
frida	v16.1.5
adb	v10.0.19045

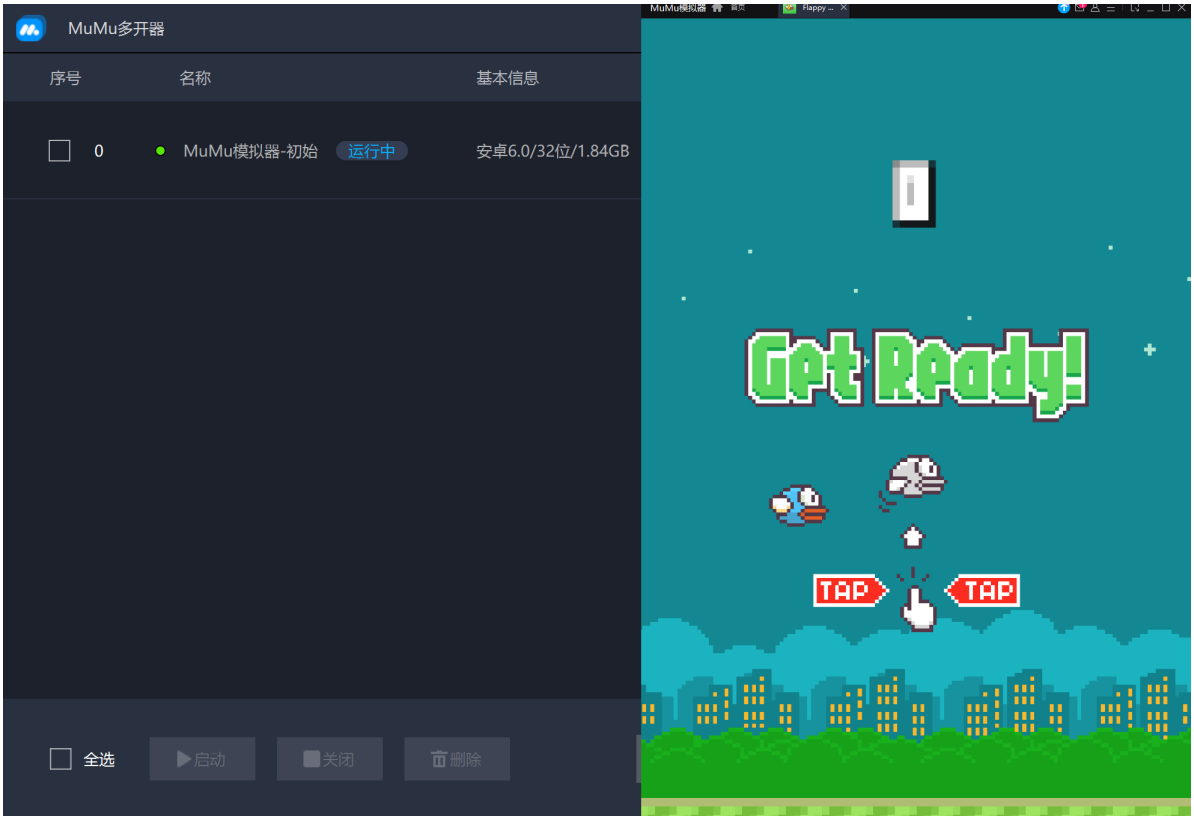
1. 对游戏APK的分析

将安装包push入MuMu12.0，发现安卓版本太高，在apkXML文件中有明确限制。

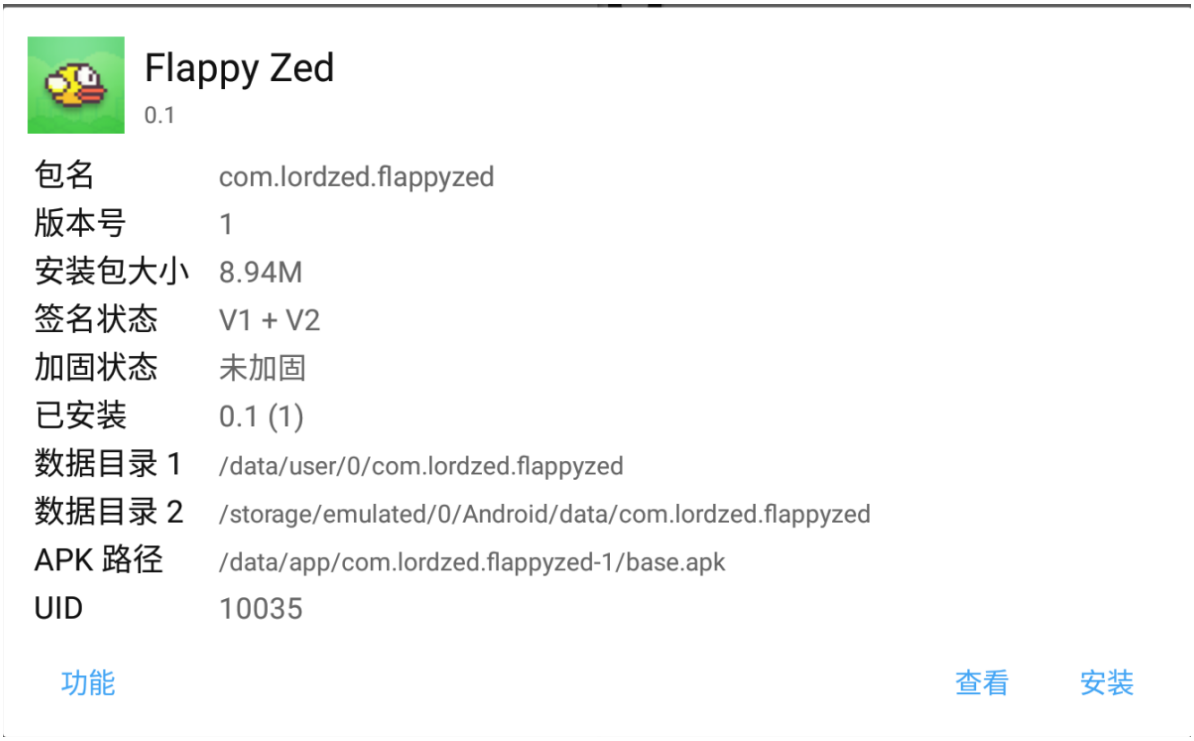
```
D:\Learning\2023project\TLearning\题目3和题目4\平仔骏-U202112052-第四次作业>adb install FlappyBird.apk
Performing Streamed Install
adb: failed to install FlappyBird.apk: Failure [INSTALL_PARSE_FAILED_MANIFEST_MALFORMED: Failed parse during installPack
ageLI: /data/app/vmdl1195189510.tmp/base.apk (at Binary XML file line #41): com.unity3d.player.UnityPlayerActivity: Targ
eting S+ (version 31 and above) requires that an explicit value for android:exported be defined when intent filters are
present]
```

故换为MuMu6.0，成功安装游戏，正常运行。

```
D:\Learning\2023project\TLearning\题目3和题目4\平仔骏-U202112052-第四次作业>adb install FlappyBird.apk
Performing Push Install
FlappyBird.apk: 1 file pushed, 0 skipped. 26.4 MB/s (9370532 bytes in 0.339s)
        pkg: /data/local/tmp/FlappyBird.apk
Success
```



用MT管理器提取安装包，包名`com.lordzed.flappyzed`未加固，继续查看其XML文件和lib动态库

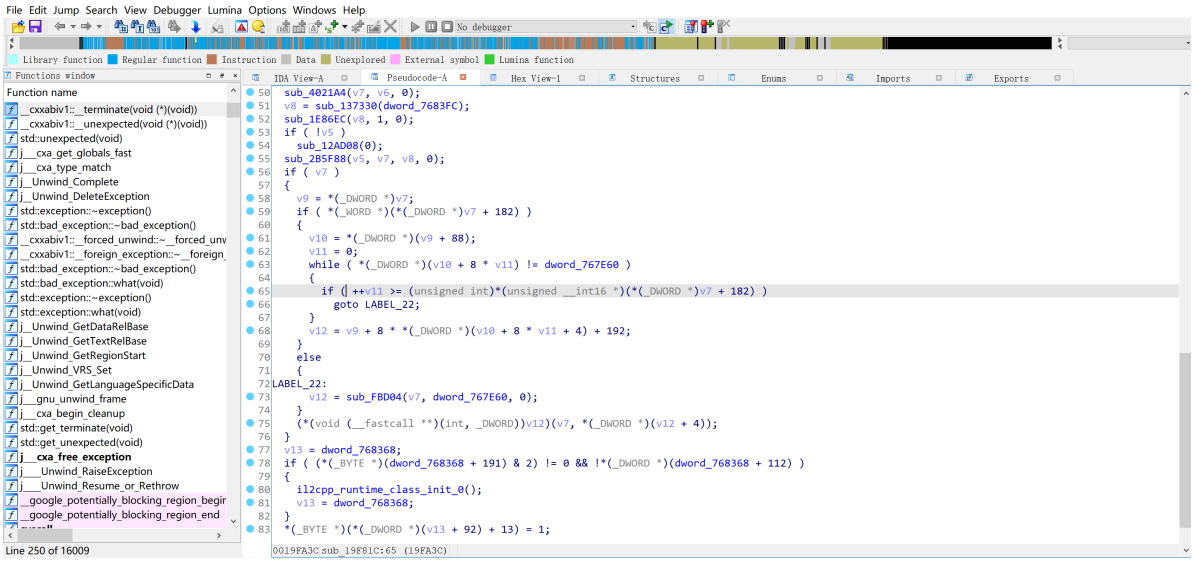


XML文件没什么有用信息，只能找到主界面`com.unity3d.player.UnityPlayerActivity`这应该是Unity游戏默认的界面名字。

```
<application
    android:theme="@7F040001"
    android:label="@7F030000"
    android:icon="@7F020000"
    android:banner="@7F010000"
    android:isGame="true">
    <activity
        android:label="@7F030000"
        android:name="com.unity3d.player.UnityPlayerActivity"
        android:launchMode="2"
        android:screenOrientation="1"
        android:configChanges="0x40003FFF"
        android:hardwareAccelerated="false">
        <intent-filter>
            <action
                android:name="android.intent.action.MAIN" />
            <category
                android:name="android.intent.category.LAUNCHER" />
            <category
                android:name="android.intent.category.LEANBACK_LAUNCHER" />
        </intent-filter>
        <meta-data
            android:name="unityplayer.UnityActivity"
            android:value="true" />
    </activity>
```

lib文件夹里颇有收获，发现`libil2cpp.so`文件，说明该游戏使用`Unity-il2cpp`框架。

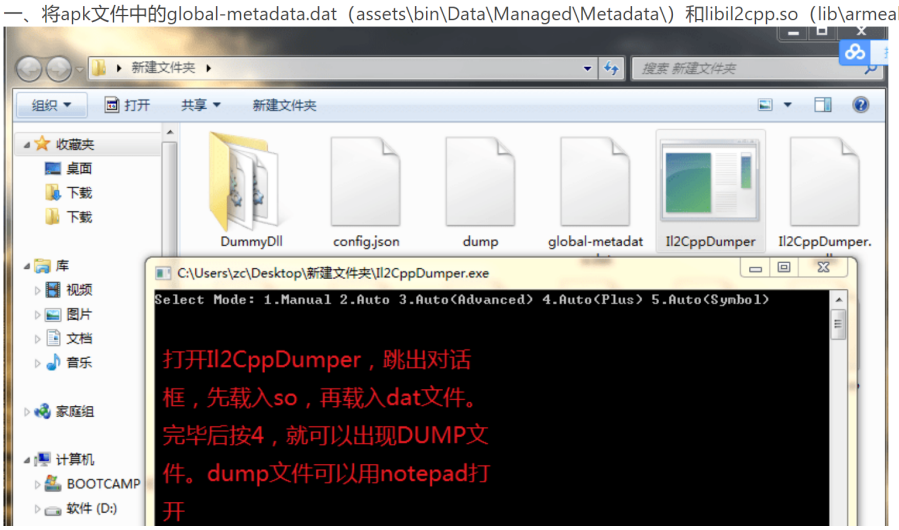
通过DIE查询，可知是32位的可执行文件，用IDA32打开，但是没有符号信息，无法直接进行静态分析



2. 基于il2CppDumper分析libil2cpp.so文件

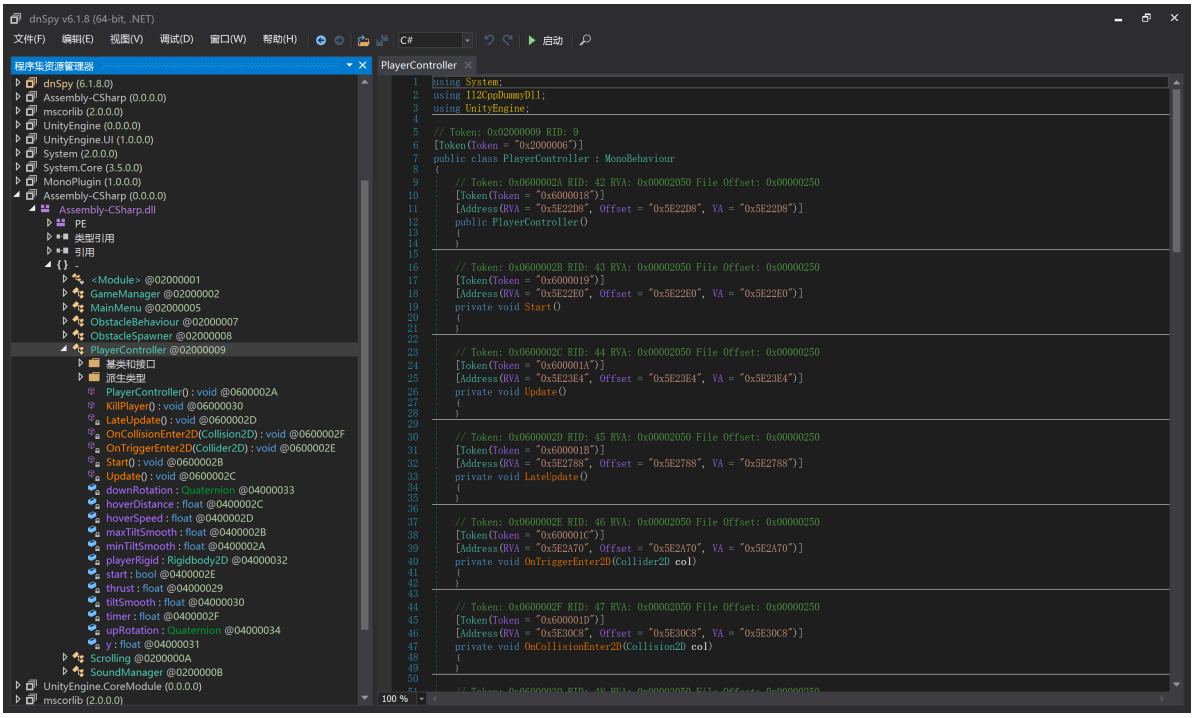
由于`IL2CPP`有静态**符号**信息泄露风险，我们可以使用IL2CPPDumper直接获取类名、方法名以及它们的偏移。根据il2CppDumper的使用教程，解压apk文件并找出想dump的so文件和dat文件。

一、将apk文件中的global-metadata.dat（assets\bin\Data\Managed\Metadata\）和libil2cpp.so（lib\armeabi-v7a\）解压到同一个文件夹中



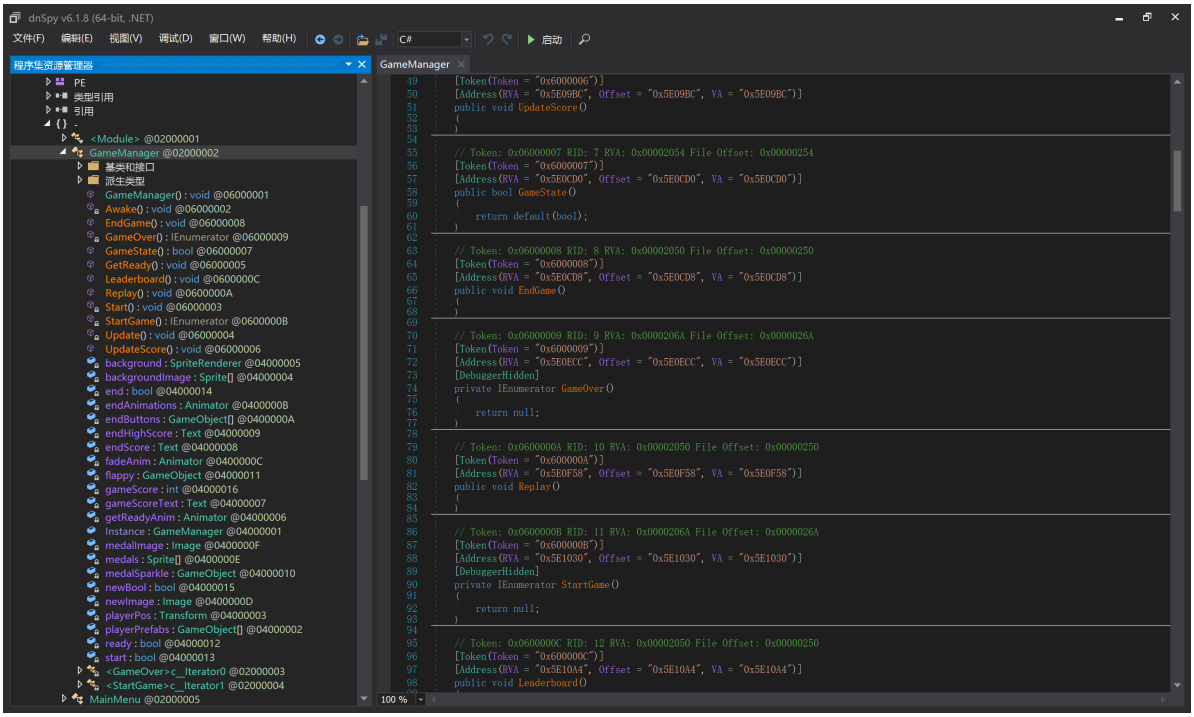

```
D:\Learning\CTF\AndroidReverse\Il2CppDumper\Il2CppDumper.exe global-metadata.dat global-metadata.dat
Select Mode: 1.Manual 2.Auto 3.Auto(Advanced) 4.Auto(Plus) 5.Auto(Symbol)
4
```

转储下来的文件很多，我们逐个分析。先关注`DummyDll`文件夹下的`Assembly-CSharp.dll`，这在windows系统下的Unity游戏中可是很重要的库文件，用`DnSpy`打开



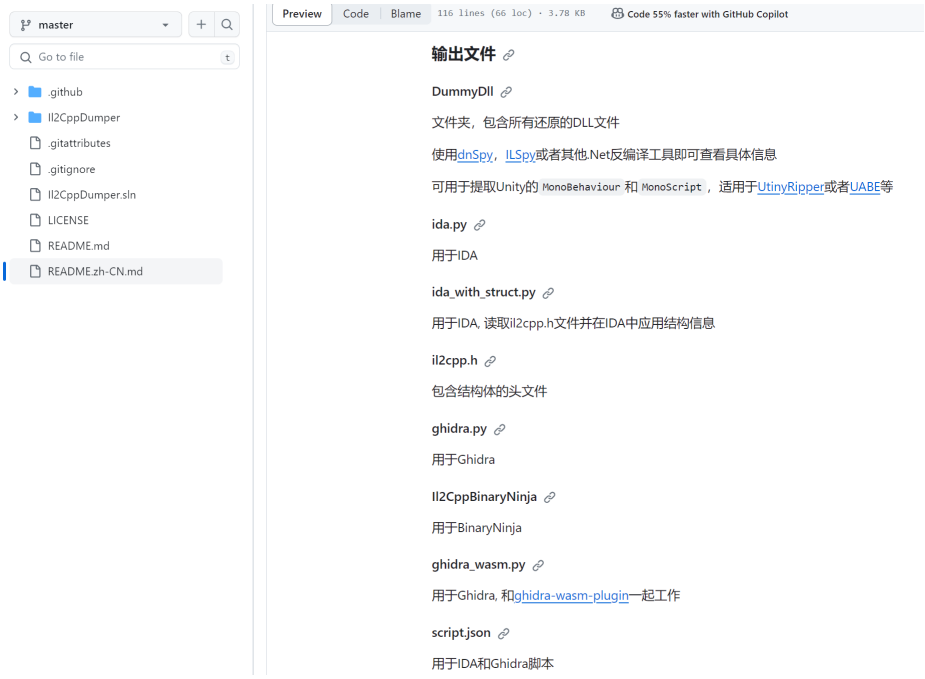
打开发现有类名也有方法名，但是里面的实现都是空的，其中`PlayerController`很明显是控制玩家对象的类，`OnCollisionEnter2D`和`OnTriggerEnter2D`很明显是翻越管道的加分逻辑和碰撞反馈的逻辑函数，后面应该会重点研究。

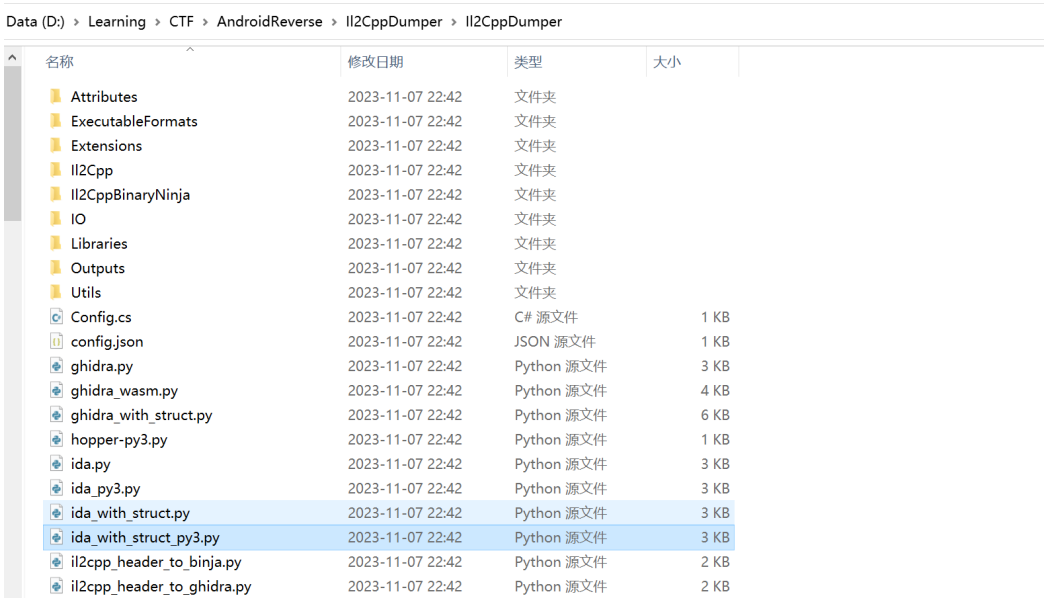
通过右侧去掉实现内容的代码信息中，也能观察到每个成员的**偏移地址**，后面可能会用到。



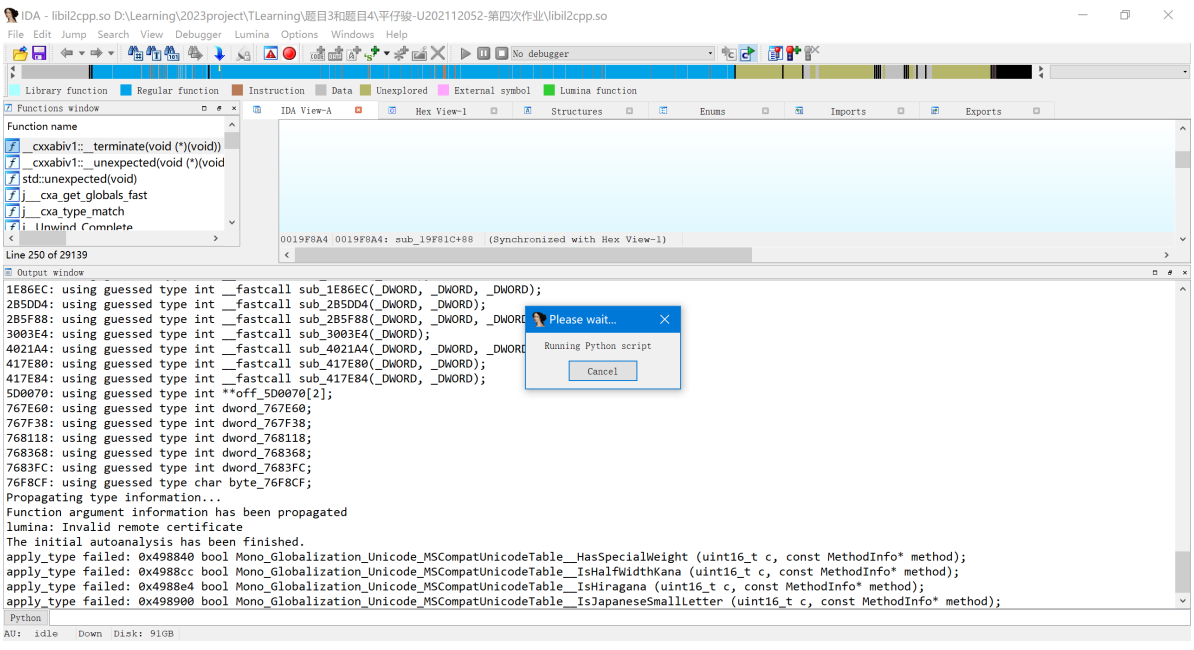
`GameManager`类同样需要重点关注，因为里面有许多控制分数和游戏状态的逻辑，如`Update`、`UpdateScore`和`GameState`等方法。

接下来使用`IDA32`，结合`IL2CppDumper`仓库中现有的python脚本，恢复`il2cpp.h`中的结构体信息和`script.json`中的符号信息，从而静态分析`libil2cpp.so`文件。

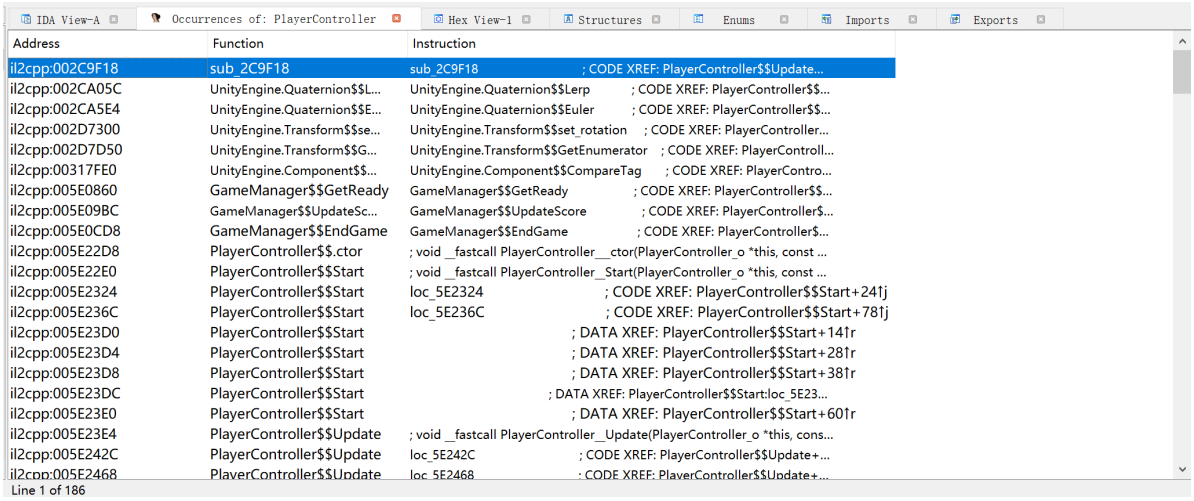




最后选择 `ida_with_struct_py3.py` 脚本：



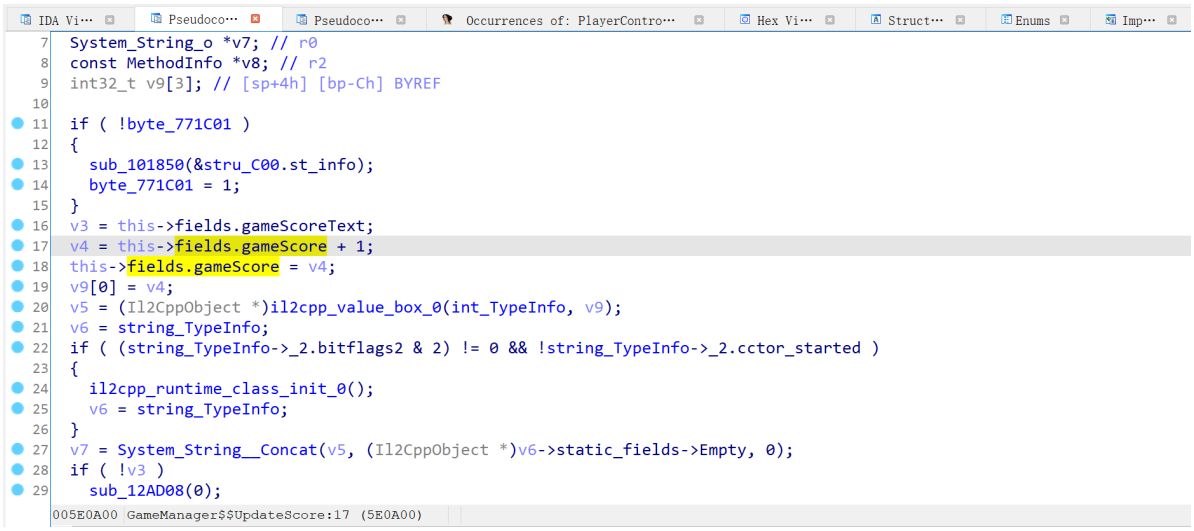
在进行符号转换的文件中搜索“PlayerController”字符串，并在结果中检索与我们需要修改游戏逻辑的几个成员属性和函数。



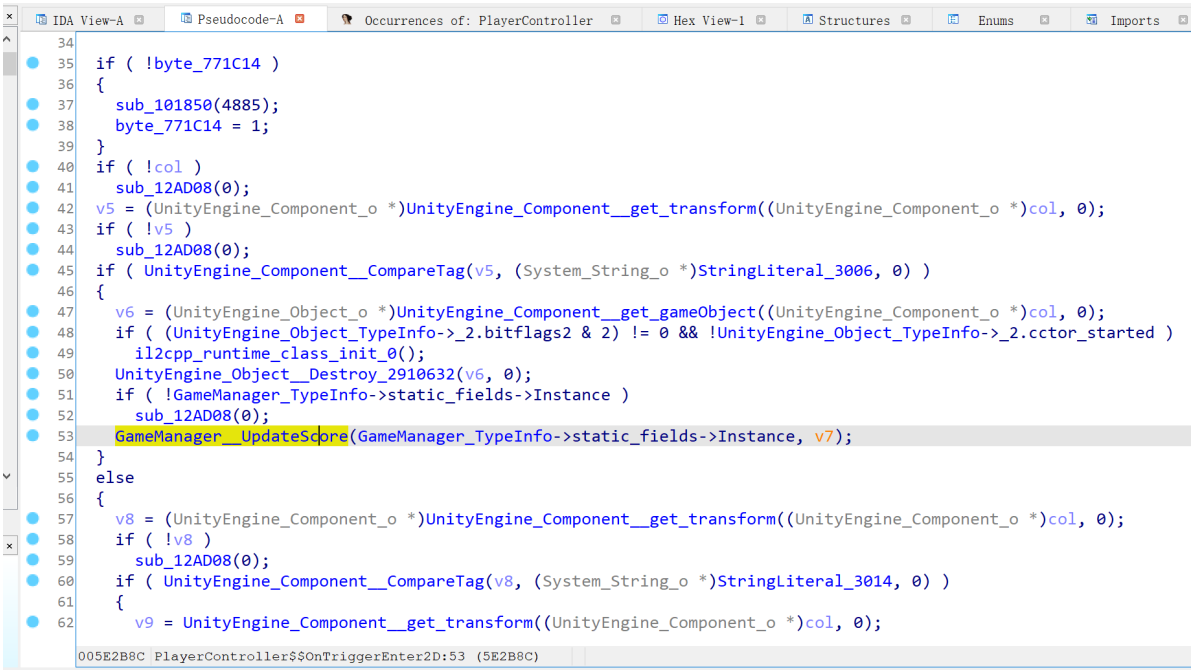
下面是更新游戏分数的逻辑。有些`StringLiteral_xxxx`的Tag我没有用脚本进行转化，这里给出部分对应表：

> 在对应表中并没有**Pipe**，只有**Obstacle**，表示障碍物，这里Obstacle应该代指Pipe

```
3004    Start
3005    Point
3006    Score
3007    GameOver
3008    Hit
3009    StartGame
3010    Swoosh
3011    End
3012    Game
3013    Flap
3014    Obstacle
3015    Ground
```

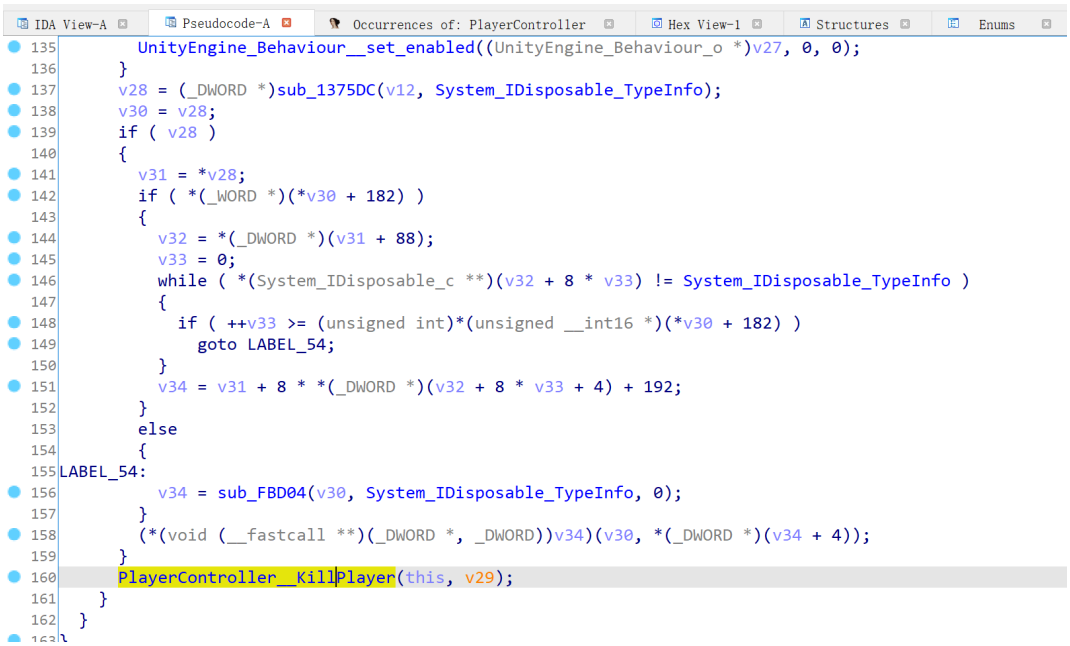


下面是`OnTriggerEnter2D`的反编译代码，可以看出是游戏结束时的触发逻辑，在游戏结束时更新分数，最后还会`KillPlayer`！



```
 34
 35  if ( !byte_771C14 )
 36  {
 37    sub_101850(4885);
 38    byte_771C14 = 1;
 39  }
 40  if ( !col )
 41    sub_12AD08(0);
 42  v5 = (UnityEngine_Component_o *)UnityEngine_Component__get_transform((UnityEngine_Component_o *)col, 0);
 43  if ( !v5 )
 44    sub_12AD08(0);
 45  if ( UnityEngine_Component__CompareTag(v5, (System_String_o *)StringLiteral_3006, 0) )
 46  {
 47    v6 = (UnityEngine_Object_o *)UnityEngine_Component__get_gameObject((UnityEngine_Component_o *)col, 0);
 48    if ( (UnityEngine_Object_TypeInfo->_2.bitflags2 & 2) != 0 && !UnityEngine_Object_TypeInfo->_2.cctor_started )
 49      il2cpp_runtime_class_init_0();
 50    UnityEngine_Object__Destroy_2910632(v6, 0);
 51    if ( !GameManager_TypeInfo->static_fields->Instance )
 52      sub_12AD08(0);
 53    GameManager__UpdateScore(GameManager_TypeInfo->static_fields->Instance, v7);
 54  }
 55  else
 56  {
 57    v8 = (UnityEngine_Component_o *)UnityEngine_Component__get_transform((UnityEngine_Component_o *)col, 0);
 58    if ( !v8 )
 59      sub_12AD08(0);
 60    if ( UnityEngine_Component__CompareTag(v8, (System_String_o *)StringLiteral_3014, 0) )
 61    {
 62      v9 = UnityEngine_Component__get_transform((UnityEngine_Component_o *)col, 0);
```

005E2B8C PlayerController$$OnTriggerEnter2D:53 (5E2B8C)



```
135        UnityEngine_Behaviour__set_enabled((UnityEngine_Behaviour_o *)v27, 0, 0);
136      }
137      v28 = (_DWORD *)sub_1375DC(v12, System_IDisposable_TypeInfo);
138      v30 = v28;
139      if ( v28 )
140      {
141        v31 = *v28;
142        if ( *(_WORD *)(*v30 + 182) )
143        {
144          v32 = *(_DWORD *)(v31 + 88);
145          v33 = 0;
146          while ( *(System_IDisposable_c **)(v32 + 8 * v33) != System_IDisposable_TypeInfo )
147          {
148            if ( ++v33 >= (unsigned int)*(unsigned __int16 *)(*v30 + 182) )
149              goto LABEL_54;
150          }
151          v34 = v31 + 8 * *(_DWORD *)(v32 + 8 * v33 + 4) + 192;
152        }
153        else
154        {
155LABEL_54:
156          v34 = sub_FBD04(v30, System_IDisposable_TypeInfo, 0);
157        }
158        (*(void (__fastcall **)(_DWORD *, _DWORD))v34)(v30, *(_DWORD *)(v34 + 4));
159      }
160      PlayerController__KillPlayer(this, v29);
161    }
162  }
```

下面是`OnCollisionEnter2D`的反编译代码，可以看出这里主要判断与地面的碰撞

```
 12  if ( !byte_771C15 )
 13  {
 14    sub_101850(&stru_1310.st_value);
 15    byte_771C15 = 1;
 16  }
 17  if ( !col )
 18    sub_12AD08(0);
 19  v5 = (UnityEngine_Component_o *)UnityEngine_Collision2D__get_transform(col, 0);
 20  if ( !v5 )
 21    sub_12AD08(0);
 22  if ( UnityEngine_Component__CompareTag(v5, (System_String_o *)String_Ground, 0) )
 23  {
 24    if ( !this->fields.playerRigid )
 25      sub_12AD08(0);
 26    UnityEngine_Rigidbody2D__set_simulated(this->fields.playerRigid, 0, 0);
 27    PlayerController__KillPlayer(this, v6);
 28    v7 = UnityEngine_Component__get_transform((UnityEngine_Component_o *)this, 0);
 29    v8 = this->fields.downRotation.fields.x;
 30    v9 = this->fields.downRotation.fields.y;
 31    v10 = this->fields.downRotation.fields.z;
 32    v11 = this->fields.downRotation.fields.w;
 33    if ( !v7 )
 34      sub_12AD08(0);
 35    v12.fields.x = v8;
 36    *(_QWORD *)&v12.fields.y = __PAIR64__(LODWORD(v10), LODWORD(v9));
 37    v12.fields.w = v11;
 38    UnityEngine_Transform__set_rotation(v7, v12, 0);
 39  }
 40}
```

005E3148 PlayerController$$OnCollisionEnter2D:22 (5E3148)

3. 实战外挂实现

3.1 直接修改so文件

回顾上面找到的3个关键方法函数，只需要用IDA Pro进行一些Patch就可以实现外挂。

- Patch分数更新逻辑，使得一次跳跃就能加255分！

```
il2cpp:005E09FC
il2cpp:005E09FC                 loc_5E09FC                              ; CODE XREF: GameManager$$UpdateScore+20↑j
il2cpp:005E09FC E4 00 9F E5                 LDR             R0, =(off_75869C - 0x5E0A10)
il2cpp:005E0A00 50 10 95 E5                 LDR             R1, [R5,#0x50]
il2cpp:005E0A04 20 40 95 E5                 LDR             R4, [R5,#0x20]
il2cpp:005E0A08 00 00 9F E7                 LDR             R0, [PC,R0] ; off_75869C ; int_TypeInfo
il2cpp:005E0A0C FF 10 81 E2                 ADD             R1, R1, #0xFF ; 分数更新
il2cpp:005E0A10 50 10 85 E5                 STR             R1, [R5,#0x50]
il2cpp:005E0A14 04 10 8D E5                 STR             R1, [SP,#0x10+var_C]
il2cpp:005E0A18 04 10 8D E2                 ADD             R1, SP, #0x10+var_C
il2cpp:005E0A1C 00 00 90 E5                 LDR             R0, [R0] ; int_TypeInfo
il2cpp:005E0A20 1D 5A ED EB                 BL              il2cpp_value_box_0
il2cpp:005E0A24 00 50 A0 E1                 MOV             R5, R0
il2cpp:005E0A28 BC 00 9F E5                 LDR             R0, =(off_75833C - 0x5E0A34)
il2cpp:005E0A2C 00 00 9F E7                 LDR             R0, [PC,R0] ; off_75833C ; string_TypeInfo
il2cpp:005E0A30 00 00 90 E5                 LDR             R0, [R0] ; string_TypeInfo
il2cpp:005E0A34 BF 10 D0 E5                 LDRB            R1, [R0,#0xBF]
il2cpp:005E0A38 02 00 11 E3                 TST             R1, #2
il2cpp:005E0A3C 06 00 00 0A                 BEQ             loc_5E0A5C
il2cpp:005E0A40 70 10 90 E5                 LDR             R1, [R0,#0x70]
il2cpp:005E0A44 00 00 51 E3                 CMP             R1, #0
il2cpp:005E0A48 03 00 00 1A                 BNE             loc_5E0A5C
```

- Patch `OnTrigger` 碰撞逻辑，使得即使撞到了障碍物也不会跳到 `KillPlayer` 逻辑，由于两次比较的Tag分别为 `GameOver` 和 `Obstacle` ，需要将第二次分支判断Patch掉才能达到无敌的效果。

> 游戏结束也分为成功结束和失败结束，这个方法用一个嵌套的方式编写可能就是为了区分是通关后的GameOver还是碰撞了Obstacle后的GameOver

```
45  if ( UnityEngine_Component__CompareTag(v5, (System_String_o *)GameOver, 0) )
46  {
47    v6 = (UnityEngine_Object_o *)UnityEngine_Component__get_gameObject((UnityEngine_Component_o *)col, 0);
48    if ( (UnityEngine_Object_TypeInfo->_2.bitflags2 & 2) != 0 && !UnityEngine_Object_TypeInfo->_2.cctor_started )
49      il2cpp_runtime_class_init_0();
50    UnityEngine_Object__Destroy_2910632(v6, 0);
51    if ( !GameManager_TypeInfo->static_fields->Instance )
52      sub_12AD08(0);
53    GameManager__UpdateScore(GameManager_TypeInfo->static_fields->Instance, v7);
54  }
55  else
56  {
57    v8 = (UnityEngine_Component_o *)UnityEngine_Component__get_transform((UnityEngine_Component_o *)col, 0);
58    if ( !v8 )
59      sub_12AD08(0);
60    if ( UnityEngine_Component__CompareTag(v8, (System_String_o *)Obstacle, 0) )
61    {
62      v9 = UnityEngine_Component__get_transform((UnityEngine_Component_o *)col, 0);
63      if ( !v9 )
64        sub_12AD08(0);
65      v10 = (UnityEngine_Component_o *)UnityEngine_Transform__get_parent(v9, 0);
```

下面是第一处判断的逻辑：

```
il2cpp:005E2AF4 06 00 A0 E1                 MOV             R0, R6  ; this
il2cpp:005E2AF8 38 D5 F4 EB                 BL              UnityEngine.Component$$CompareTag ; GameOver
il2cpp:005E2AFC 00 60 A0 E1                 MOV             R6, R0
il2cpp:005E2B00 00 00 55 E3                 CMP             R5, #0
il2cpp:005E2B04 01 00 00 1A                 BNE             loc_5E2B10
il2cpp:005E2B08 00 00 A0 E3                 MOV             R0, #0
il2cpp:005E2B0C 7D 20 ED EB                 BL              sub_12AD08
il2cpp:005E2B10             ; ---------------------------------------------------------------------------
il2cpp:005E2B10
il2cpp:005E2B10                 loc_5E2B10                              ; CODE XREF: PlayerController$$OnTriggerEnter2D+94↑j
il2cpp:005E2B10 01 00 56 E3                 CMP             R6, #1
il2cpp:005E2B14 1D 00 00 1A                 BNE             Compare_Obstacle ; GameOver的判断逻辑
il2cpp:005E2B18 05 00 A0 E1                 MOV             R0, R5  ; this
il2cpp:005E2B1C 00 10 A0 E3                 MOV             R1, #0  ; method
```

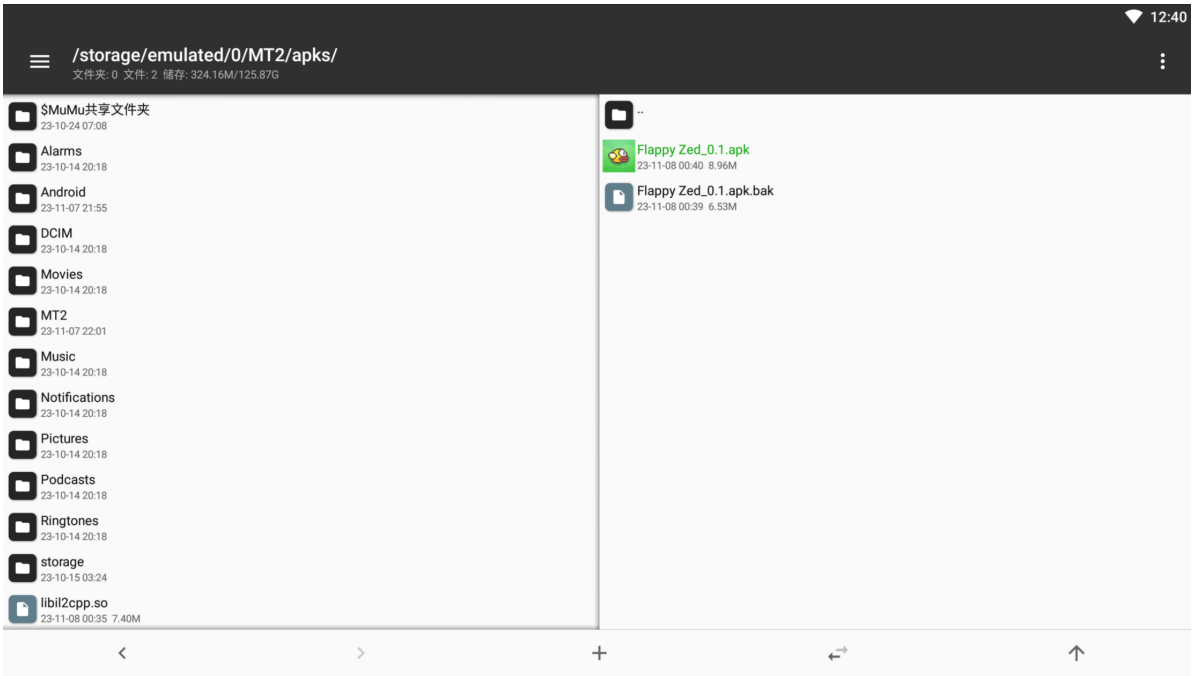
第二处判断跳转的程序段在 `KillPlayer` 之后，这说明应该在这里无条件跳转，使玩家避免死亡，我们将其patch成 `B` 也就是将操作数机器码改为 `EA`

```
il2cpp:005E2BB0                 loc_5E2BB0                              ; CODE XREF: PlayerController$$OnTriggerEnter2D+134↑j
il2cpp:005E2BB0 D0 03 9F E5                     LDR             R0, =(off_766DBC - 0x5E2BC0)
il2cpp:005E2BB4 00 20 A0 E3                     MOV             R2, #0  ; method
il2cpp:005E2BB8 00 00 9F E7                     LDR             R0, [PC,R0] ; off_766DBC ; Obstacle
il2cpp:005E2BBC 00 10 90 E5                     LDR             R1, [R0] ; tag
il2cpp:005E2BC0 06 00 A0 E1                     MOV             R0, R6  ; this
il2cpp:005E2BC4 05 D5 F4 EB                     BL              UnityEngine.Component$$CompareTag ; Obstacle
il2cpp:005E2BC8 01 00 50 E3                     CMP             R0, #1
il2cpp:005E2BCC E5 00 00 1A                     BNE             Alive   ; no kill
il2cpp:005E2BD0 00 00 55 E3                     CMP             R5, #0
il2cpp:005E2BD4 01 00 00 1A                     BNE             loc_5E2BE0
il2cpp:005E2BD8 00 00 A0 E3                     MOV             R0, #0
il2cpp:005E2BDC 49 20 ED EB                     BL              sub_12AD08
```

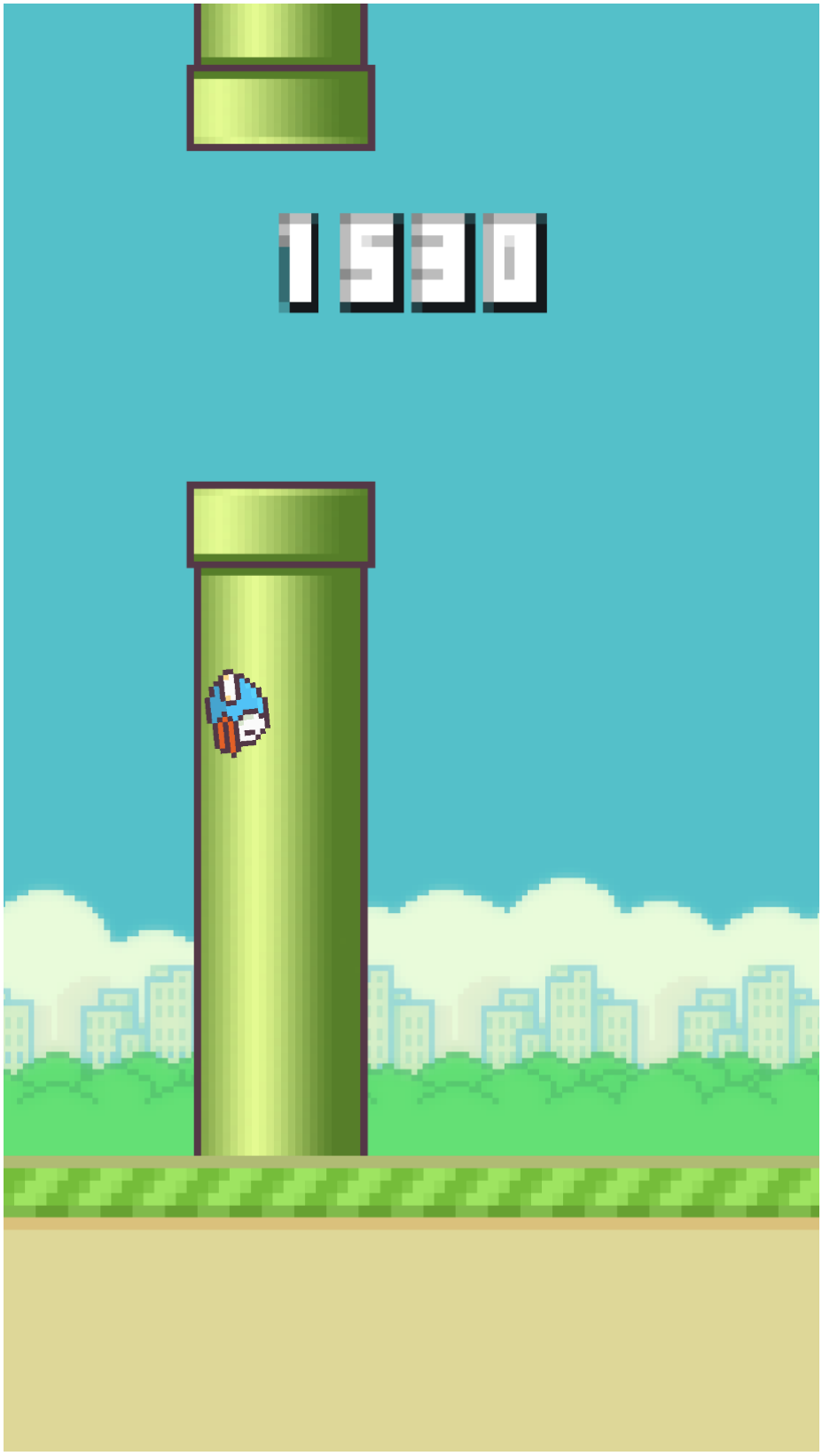
- 同上，对于触碰地面的逻辑也进行了Patch，使小鸟不会死亡。

```
il2cpp:005E313C                 loc_5E313C                              ; CODE XREF: PlayerController$$OnCollisionEnter2D+68↑j
il2cpp:005E313C A0 00 9F E5                     LDR             R0, =(off_766DD0 - 0x5E314C)
il2cpp:005E3140 00 20 A0 E3                     MOV             R2, #0  ; method
il2cpp:005E3144 00 00 9F E7                     LDR             R0, [PC,R0] ; off_766DD0 ; Ground
il2cpp:005E3148 00 10 90 E5                     LDR             R1, [R0] ; tag
il2cpp:005E314C 05 00 A0 E1                     MOV             R0, R5  ; this
il2cpp:005E3150 A2 D3 F4 EB                     BL              UnityEngine.Component$$CompareTag ; Ground
il2cpp:005E3154 01 00 50 E3                     CMP             R0, #1
il2cpp:005E3158 1C 00 00 EA                     B               Alive   ; 无条件跳转
il2cpp:005E315C                 ; ---------------------------------------------------------------------------
il2cpp:005E315C 30 50 94 E5                     LDR             R5, [R4,#0x30]
il2cpp:005E3160 00 00 55 E3                     CMP             R5, #0
il2cpp:005E3164 01 00 00 1A                     BNE             loc_5E3170
il2cpp:005E3168 00 00 A0 E3                     MOV             R0, #0
il2cpp:005E316C E5 1E ED EB                     BL              sub_12AD08
il2cpp:005E3170                 ; ---------------------------------------------------------------------------
```

将修改后的.so文件push到模拟器中，再用MT管理器重新打包。（自动重新签名）



效果如下图，小鸟已经无视碰撞事件了，并且每次翻越能加255分。



3.2 Frida脚本编写，Hook游戏实现外挂

frida-server-16.1.5-android-arm.xz	6.62 MB	3 days ago
frida-server-16.1.5-android-arm64.xz	14.8 MB	3 days ago
frida-server-16.1.5-android-x86.xz	15 MB	3 days ago
frida-server-16.1.5-android-x86_64.xz	30.2 MB	3 days ago
frida-server-16.1.5-freebsd-arm64.xz	7.39 MB	3 days ago
frida-server-16.1.5-freebsd-x86_64.xz	7.52 MB	3 days ago

将下载好的合适版本的`frida_server` push进模拟器

```
shell@x86:/ $ su
root@x86:/ # cd /data/local/tmp
root@x86:/data/local/tmp # ;ls
sh: syntax error: ';' unexpected
1|root@x86:/data/local/tmp # ls
CrackMe2
busybox
frida-server-16.1.5-android-x86
injector
libhook.so
/frida-server-16.1.5-android-x86                                    <
sh: ./frida-server-16.1.5-android-x86: can't execute: Permission denied
hmod 777 frida-server-16.1.5-android-x86                            <
root@x86:/data/local/tmp # ./frida-server-16.1.5-android-x86

root@x86:/data/local/tmp # ./frida-server-16.1.5-android-x86 -U
Unknown option -U
Run './frida-server-16.1.5-android-x86 --help' to see a full list of available command line options.
1|root@x86:/data/local/tmp # ./frida-server-16.1.5-android-x86
```

用`frida-ps -U`测试，可以正常运行

```
D:\Learning\2023project\TLearning\题目3和题目4\平仔骏-U202112052-第四次作业>adb shell getprop ro.product.cpu.abi
x86

D:\Learning\2023project\TLearning\题目3和题目4\平仔骏-U202112052-第四次作业>frida-ps -U
  PID  Name
-----  ------------------------------
17263  Flappy Zed
  245  VBoxShell
 1006  android.process.acore
  887  android.process.media
 1368  com.android.defcontainer
16198  com.android.externalstorage
16134  com.android.packageinstaller
 1430  com.android.phone
16215  com.android.shell
  788  com.android.systemui
  300  debuggerd
  302  drmserver
17387  frida-server-16.1.5-android-x86
  345  gatekeeperd
  282  healthd
    1  init
  304  installd
  305  keystore
  284  lmkd
  290  local_camera_back
  289  local_gps
17389  logcat
  143  logd
  276  logwrapper
```

编写frida插件脚本，修改在`3.1`中的几个地方的内存，即可实现外挂。

- [0x5E3158]处的shell code

```
il2cpp:005E313C             loc_5E313C                              ; CODE XREF: PlayerController$$OnCollisionEnter2D+68↑j
il2cpp:005E313C A0 00 9F E5                 LDR             R0, =(off_766DD0 - 0x5E314C)
il2cpp:005E3140 00 20 A0 E3                 MOV             R2, #0  ; method
il2cpp:005E3144 00 00 9F E7                 LDR             R0, [PC,R0] ; off_766DD0 ; Ground
il2cpp:005E3148 00 10 90 E5                 LDR             R1, [R0] ; tag
il2cpp:005E314C 05 00 A0 E1                 MOV             R0, R5  ; this
il2cpp:005E3150 A2 D3 F4 EB                 BL              UnityEngine.Component$$CompareTag ; Ground
il2cpp:005E3154 01 00 50 E3                 CMP             R0, #1
il2cpp:005E3158 1C 00 00 EA                 B               Alive   ; 无条件跳转
il2cpp:005E315C             ; ---------------------------------------------------------------------------
il2cpp:005E315C 30 50 94 E5                 LDR             R5, [R4,#0x30]
il2cpp:005E3160 00 00 55 E3                 CMP             R5, #0
il2cpp:005E3164 01 00 00 1A                 BNE             loc_5E3170
il2cpp:005E3168 00 00 A0 E3                 MOV             R0, #0
il2cpp:005E316C E5 1E ED EB                 BL              sub_12AD08
il2cpp:005E3170             ; ---------------------------------------------------------------------------
```

- [0x5E2BCC]处的shell code

```
il2cpp:005E2BB0                 loc_5E2BB0                              ; CODE XREF: PlayerController$$OnTriggerEnter2D+134↑j
il2cpp:005E2BB0 D0 03 9F E5                 LDR             R0, =(off_766DBC - 0x5E2BC0)
il2cpp:005E2BB4 00 20 A0 E3                 MOV             R2, #0  ; method
il2cpp:005E2BB8 00 00 9F E7                 LDR             R0, [PC,R0] ; off_766DBC ; Obstacle
il2cpp:005E2BBC 00 10 90 E5                 LDR             R1, [R0] ; tag
il2cpp:005E2BC0 06 00 A0 E1                 MOV             R0, R6  ; this
il2cpp:005E2BC4 05 D5 F4 EB                 BL              UnityEngine.Component$$CompareTag ; Obstacle
il2cpp:005E2BC8 01 00 50 E3                 CMP             R0, #1
il2cpp:005E2BCC E5 00 00 1A                 BNE             Alive   ; no kill
il2cpp:005E2BD0 00 00 55 E3                 CMP             R5, #0
il2cpp:005E2BD4 01 00 00 1A                 BNE             loc_5E2BE0
il2cpp:005E2BD8 00 00 A0 E3                 MOV             R0, #0
il2cpp:005E2BDC 49 20 ED EB                 BL              sub_12AD08
```

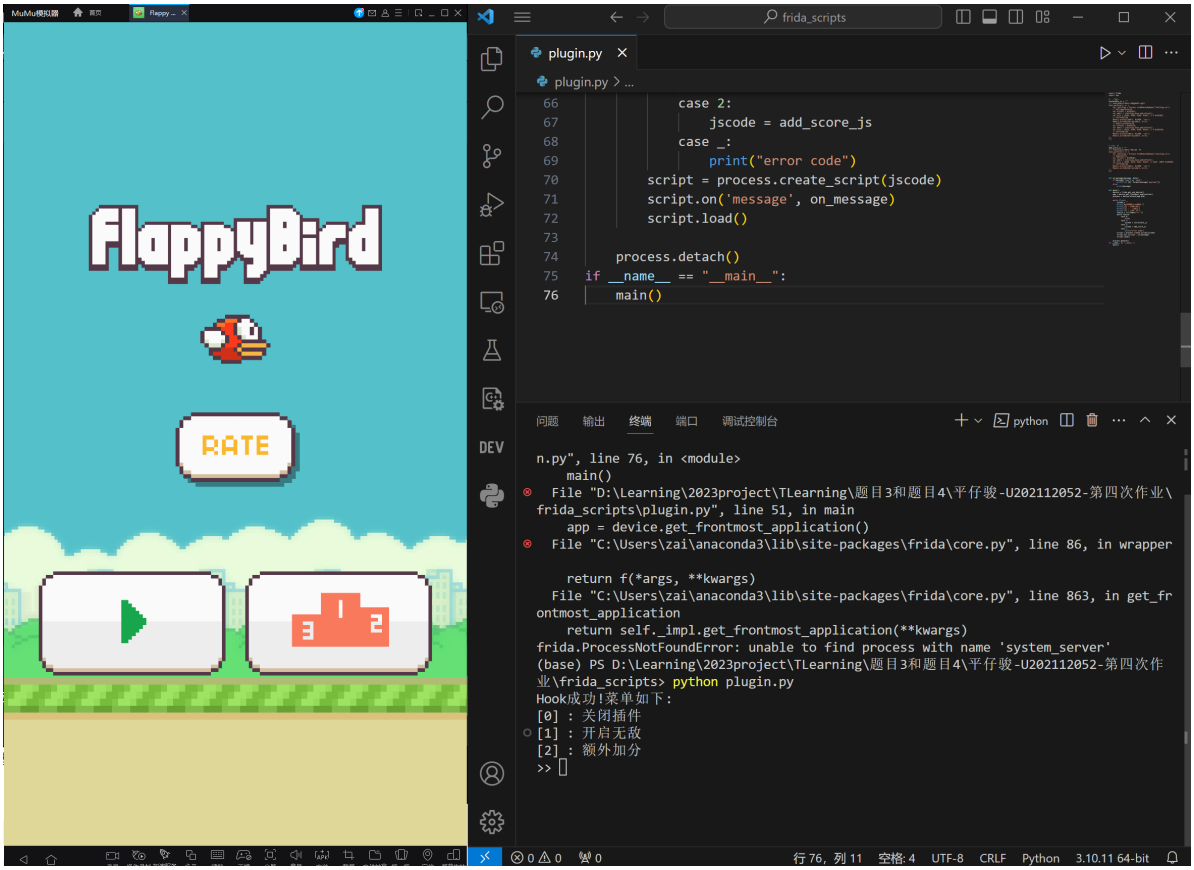
- [0x5E0A0C]处的shell code

```
il2cpp:005E09FC
il2cpp:005E09FC                 loc_5E09FC                              ; CODE XREF: GameManager$$UpdateScore+20↑j
il2cpp:005E09FC E4 00 9F E5                 LDR             R0, =(off_75869C - 0x5E0A10)
il2cpp:005E0A00 50 10 95 E5                 LDR             R1, [R5,#0x50]
il2cpp:005E0A04 20 40 95 E5                 LDR             R4, [R5,#0x20]
il2cpp:005E0A08 00 00 9F E7                 LDR             R0, [PC,R0] ; off_75869C ; int_TypeInfo
il2cpp:005E0A0C FF 10 81 E2                 ADD             R1, R1, #0xFF ; 分数更新
il2cpp:005E0A10 50 10 85 E5                 STR             R1, [R5,#0x50]
il2cpp:005E0A14 04 10 8D E5                 STR             R1, [SP,#0x10+var_C]
il2cpp:005E0A18 04 10 8D E2                 ADD             R1, SP, #0x10+var_C
il2cpp:005E0A1C 00 00 90 E5                 LDR             R0, [R0] ; int_TypeInfo
il2cpp:005E0A20 1D 5A ED EB                 BL              il2cpp_value_box_0
il2cpp:005E0A24 00 50 A0 E1                 MOV             R5, R0
il2cpp:005E0A28 BC 00 9F E5                 LDR             R0, =(off_75833C - 0x5E0A34)
il2cpp:005E0A2C 00 00 9F E7                 LDR             R0, [PC,R0] ; off_75833C ; string_TypeInfo
il2cpp:005E0A30 00 00 90 E5                 LDR             R0, [R0] ; string_TypeInfo
il2cpp:005E0A34 BF 10 D0 E5                 LDRB            R1, [R0,#0xBF]
il2cpp:005E0A38 02 00 11 E3                 TST             R1, #2
il2cpp:005E0A3C 06 00 00 0A                 BEQ             loc_5E0A5C
il2cpp:005E0A40 70 10 90 E5                 LDR             R1, [R0,#0x70]
il2cpp:005E0A44 00 00 51 E3                 CMP             R1, #0
il2cpp:005E0A48 03 00 00 1A                 BNE             loc_5E0A5C
```

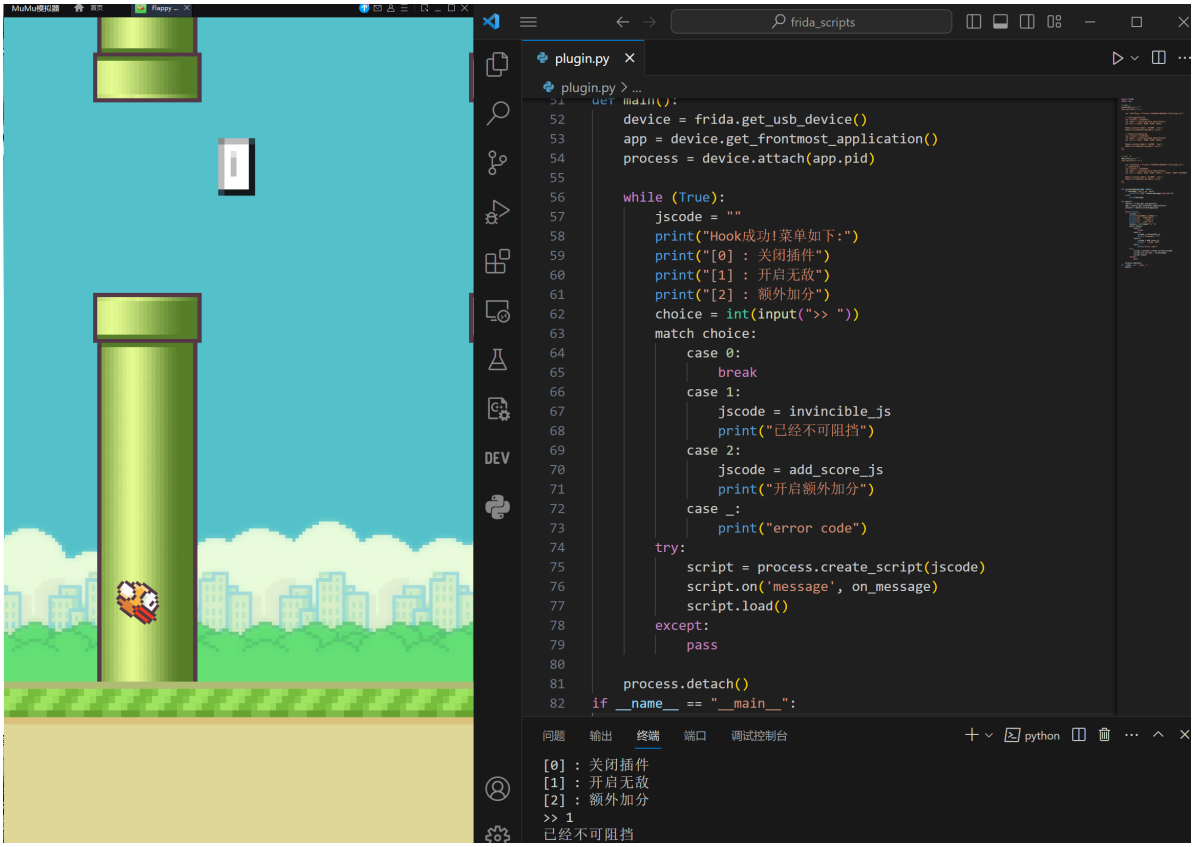
```
/// 以下脚本可以实现无视碰撞无敌
Java.perform(() => {
    var libil2cpp = Process.findModuleByName("libil2cpp.so");
    // OnTriggerEnter2D
    var offset1 = 0x5E2BCC;
    var addr1 = libil2cpp.base.add(offset1);
    var arr1 = [0xE5, 0x00, 0x00, 0xEA]; // B 0x5E2BCC
    // 修改内存保护
    Memory.protect(addr1, 0x1000, 'rwx');
    Memory.writeByteArray(addr1, arr1);
    // OnCollisionEnter2D
    var offset2 = 0x5E3158;
    var addr2 = libil2cpp.base.add(offset2);
    var arr2 = [0x1A, 0x00, 0x00, 0xEA]; // B 0x5E3158
    // 修改内存保护
    Memory.protect(addr2, 0x1000, 'rwx');
    Memory.writeByteArray(addr2, arr2);
});
```

```
/// 以下脚本可以实现额外加分
Java.perform(() => {
    var libil2cpp = Process.findModuleByName("libil2cpp.so");
    // UpdateScore
    var offset1 = 0x5E0A0C;
    var addr1 = libil2cpp.base.add(offset1);
    var arr1 = [0x64, 0x10, 0x81, 0xE2]; // 0x64加100分 0x5E0A0C
    // 修改内存保护
    Memory.protect(addr1, 0x1000, 'rwx');
    Memory.writeByteArray(addr1, arr1);
});
```

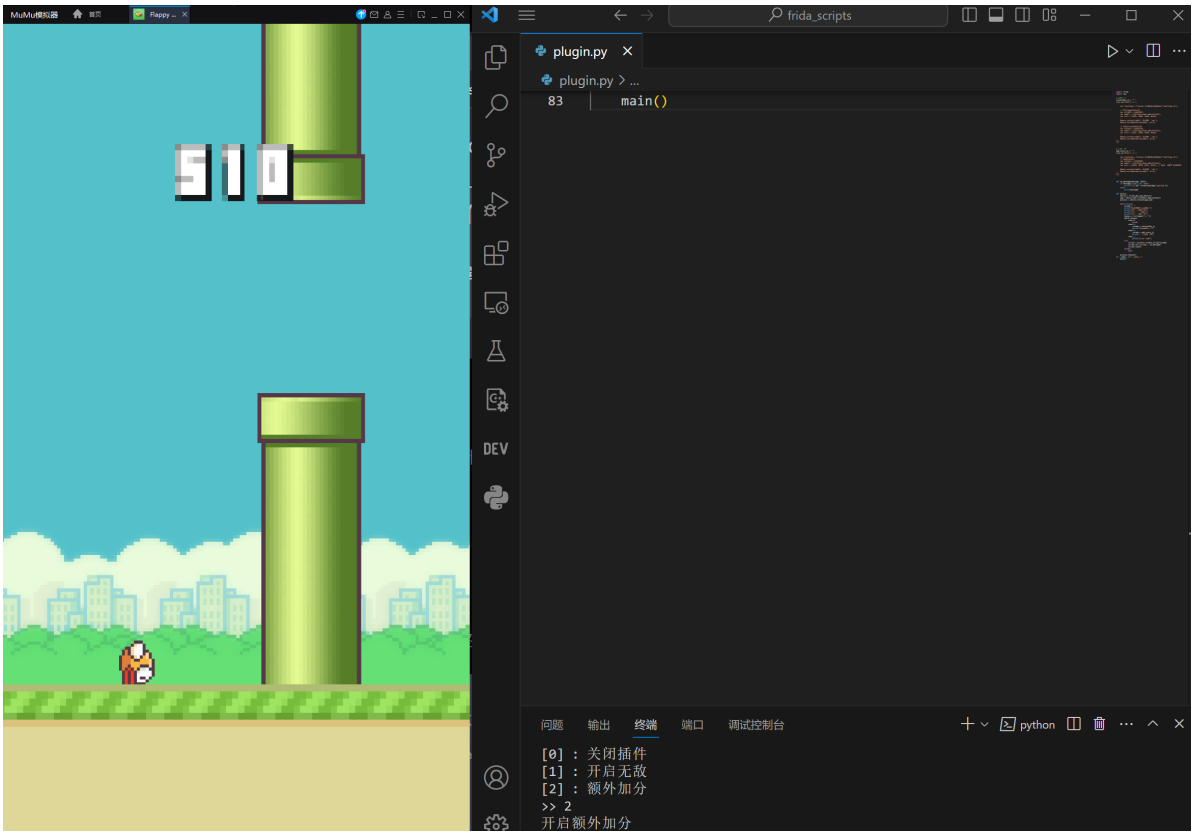
下面是连接上frida_server后启动脚本的效果



开启invincible无法阻挡



开启add_score额外加分


MuMu模拟器
Flappy ...
510
frida_scripts
plugin.py
plugin.py > ...
83 main()
DEV
问题
输出
终端
端口
调试控制台
python
[0] : 关闭插件
[1] : 开启无敌
[2] : 额外加分
>> 2
开启额外加分